PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense Component:

Department of the Army, Army National Guard and Army Reserves

2. Name of Information Technology System:

Reserve Component Automation System (RCAS)

3. Budget System Identification Number (SNAP-IT Initiative Number):

1640

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):

75

5. IT Investment (OMB Circular A-11) Unique Identifier (from IT-43/FOIT Database -- if applicable):

007-21-01-25-01-1640-00-201-067

6. Privacy Act System of Records Notice Identifier:

A0600-8aDAPE Major Command Military Personnel Management Reporting System (July 26, 2001, 66 FR 39027)
A0715-9 DCS, G-4: Support Personnel Deployment Records (January 28, 2008, 73 FR 4853)

7. OMB Information Collection Requirement Number and Expiration Date:

N/A

8. Type of authority to collect information (statutory or otherwise):

10 U.S.C. 3013, Secretary of the Army;
P. L. 108-375, Section 1205 and 1206;
Army Regulation 600-8-6, Personnel Accounting and Strength Reporting;
Army Regulation 600-8, Military Personnel Management; and
E.O. 9397 (SSN).

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup):

The RCAS is an automated information system that imports personally identifiable

information (PII) from external sources to provide the Army the capability to administer, manage, and mobilize Army Guard and Reserve forces more effectively. The mission of the RCAS is to provide the Army Reserve Components forces with an automated information system (AIS) that will accomplish day-to-day administrative tasks and provide timely, accurate, and assured information necessary to facilitate full-scale deployment management for mobilization of forces.

The proponent for RCAS is the Army National Guard and Army Reserves; the system is managed by the offices of the Assistant Secretary of the Army for Acquisition, Logistics and Technology, and the Program Executive Officer for Enterprise Information Systems.

An RCAS installation consists of a web server (which has a data exchange application and a set of RCAS web applications), and an Integrated Database (IDB). Users interact with the RCAS via the web applications. Information is exchanged with RCAS by using one of following secure methods: secure Oracle to Oracle database link, Hypertext Transport Protocol using Secure Sockets Layer (HTTPS) or Secure Shell (SSH). In some instances, data transfers between the RCAS and some of its associated Information Exchanges (IEs) are transmitted via the File Transfer Protocol (FTP). These IEs are designated as low risk because they transmit internally within the Local Area Network (LAN) enclave at the site. Proper access controls on the network and system, including local physical and standard operating procedures, are established to mitigate the risk.

More than 50 percent of the Army's force structure is in the Reserve Component. RCAS provides an integrated capability that supports mobilization and improves day-to-day administration and management of Reserve and Guard forces. RCAS links approximately 10,500 Guard and Reserve units at approximately 4,000 sites located in 50 states, three territories and the District of Columbia.

RCAS does not have the responsibility to check to verify if the ARNG and USAR are doing routine backups. Each site is responsible for ensuring its RCAS system is backed up regularly. The RCAS accreditation documentation provides guidance to the ARNG and USAR on the proper backup, storage and retention procedures.

The subordinate elements of the RCAS are:
Integrated Data Viewer – Personnel (IDV-P)
Unit Personnel System / Command Management System (UPS/CMS)
Mobilization Data Planning Viewer (MPDV)
Retirement Points Accounts Management (RPAM)
Safety Occupational Health (SOH)

10. Identifiable Information to be Collected, its Nature and Source

The following PII data is collected from Information Exchanges with external systems: name, social security number (SSN), date of birth (DoB), address, phone, race, phone, gender, Health Insurance Portability and Accountability Act (HIPAA) data. Information Exchange agreements are reviewed and updated periodically to ensure that requirements are up to date and that RCAS receives accurate data.

11. Method of Information Collection:

Information in this system is derived from data contained in other systems. Users interact with the RCAS via the web applications. This information is gathered from a number of sources including information exchanges with other Army and DoD systems. Some systems access data on non-military personnel, such as medical information on spouses.

12. Purpose of Collection and How Identifiable Information/Data will be Used:

Identifiable data will be used to support individual identification of soldiers in the mobilization, force authorization, personnel, and safety applications of the RCAS; to select soldiers for readiness in mobilization, assign individual weapons, view personal detail information, update individual and group training, accident review duties, identify individuals for promotions and transfers; search criteria and skills in order to identify and select soldiers for mobilization; reconcile personnel losses and prepare personnel lists for mobilization; and to update retirement information.

13. Does system create new data about individuals through aggregation? The system does not create or derive new PII data about individuals.

Yes, for example, RCAS applications derive soldier readiness status and mobilization eligibility based on data regarding skills, availability, training and other criteria. Based on PII data obtained through information exchanges, RCAS applications derive maintenance of retirement point accounts of individual soldiers, generation of reports to use in monitoring and improving the safety of workplaces and protecting the health of employees, and processing personnel action requests.

14. Internal and External Information/Data Sharing:

Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system. Other organizations receiving and providing data are: Defense Finance and Accounting Service (DFAS), United States Army Medical Command (MEDCOM), Assistant Secretary of the Army for Manpower and Reserve Affairs, Office of the Surgeon General, US Army Reserve Command, National Guard Bureau, Deputy Chief of Staff for Operations, United States Army Training and Doctrine Command (TRADOC), US Joint Forces Command, US Army Forces Command.

15. Opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted:

Since individuals do not provide information directly to RCAS, they are given no opportunity to object to its collection and use in RCAS. That opportunity would have had to be provided by the source system that collected information from the individual. The

opportunity to object or consent would have been provided to the individual when information was initially collected.

16. Information Provided to the Individual, the Format, and the Means of Delivery:

Individuals are provided orders for assignment and travel based on information derived from within the system.

17. Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

The RCAS Project Director has oversight of the system and ensures that it meets all applicable government, Department of Defense (DoD), and Army policies and regulations, including PII and Information Assurance (IA) requirements. The system is accessed through Army Knowledge Online (AKO), which means several layers of authentication are required in order to access the system. First, a user must login and be authenticated to AKO. Second, RCAS will validate that the user is permitted access to RCAS. Third, RCAS will assign the user the roles designated to that user. A user who does not have an assigned role is not authorized to access PII.

All information is sent using one of following secure methods: Secure Oracle to Oracle database link, Hypertext Transport Protocol using Secure Sockets Layer (HTTPS) or Secure Shell (SSH). In some instances, data transfers between the RCAS and some of its associated Information Exchanges (IEs) are transmitted via the File Transfer Protocol (FTP). These IEs are designated as low risk because they internally transmitted within the Local Area Network (LAN) enclave at the site. Both proper access controls on the network and system including local physical and standard operating procedures are established to mitigate the risk.

This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

Administrative, business, and physical protections are the responsibility of each site. Each site must comply with all applicable Department of Defense and Army Regulations.

Technical controls are documented in the DIACAP package and show that RCAS conforms to applicable controls in DoD and Army Regulations.

18. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures:

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There is no risk in providing individual the opportunity to object or consent,

Printed output from the system is appropriately marked and tracked to ensure that it is exposed only to those that are authorized to view the PII. Once the information is no

longer needed, those prints are disposed of securely.

19. Classification and Publication of Privacy Impact Assessment:

The data in the system is For Official Use Only. The PIA may be published in full.